

response to the nonce to a base station. This way, the main processor is prevented from bypassing the TEE in establishing the D2D session in case the D2D session can only be established with permission from a base station. In case the message doesn't comprise an instruction to intercept contents of the D2D session, the message may be effectively a dummy message. The dummy message may still comprise the nonce which may be handled identically to the case where the instruction to intercept is present, to conceal possible interception. In other words, the message as such may be a compulsory element of D2D session establishment, and from the point of view of the main processor, the message may be handled identically irrespective of whether or not it comprises an instruction to intercept.

[0029] In some embodiments, a main processor may perform the actions discussed herein as occurring in a TEE. This may occur, for example, if a mobile doesn't have a TEE or where a TEE isn't configured to participate in interception.

[0030] The mobile receiving the message may verify the message originates from a source authorized to issue instructions concerning interception. This verifying may comprise verifying a digital signature of the message using a signature verification key securely stored in the mobile, for example in a TEE. The TEE may perform the verifying, or alternatively the main processor may perform the verifying before providing the message to the TEE.

[0031] During a D2D session that is intercepted, the contents of the D2D session may be routed via the TEE to enable the TEE to at least in part copy the contents. The routing of the content via the TEE may occur regardless of whether actual intercepting takes place, to conceal any interception from a user of the terminal and/or the main operating system of the mobile. In case encryption is used in the D2D session and a main processor of the mobile performs the encryption and decryption, the routing of the content via the TEE may involve routing of a decrypted version of the content.

[0032] When the mobile provides, as part of intercepting, a copy containing at least part of the contents of the D2D session to a base station it may provide it in encrypted form. To enable this, the mobile, for example a TEE comprised in the mobile, may be in possession of an encryption key to use before providing the copy of the content toward a base station. The encryption key may be statically stored in the mobile, or the encryption key may be provided in the message comprising an instruction to perform the intercepting. In the latter case, the message may be arranged to be of the same length regardless of whether it comprises the instruction to intercept and the key, or not. Providing the contents in encrypted form may be desirable in case the contents involve private information, such as for example contents of a telephone discussion.

[0033] A TEE may be configured to process the contents of the D2D session before transmitting it to a base station. For example, if the D2D session is a telephone call, the TEE may be configured to perform speech recognition on the contents and provide a transcript of the telephone call instead of audio data of the call. This may reduce the amount of data to be provided as content, which may reduce battery consumption when transmitting and may also reduce the likelihood that a user of the mobile notices the transmission. Another example of processing is where the contents are compressed by using a compression algorithm. A yet further example is where only part of the contents are copied in the interception. For example, if the D2D session is a video call, the message

comprising the instruction to intercept may specify that the interception is only to apply to audio, not video. In general where the D2D session comprises multiple media elements, the message may specify which media elements are to be subject to interception.

[0034] In general there is provided an apparatus, such as for example a mobile, a control device for inclusion in a mobile, to control the functioning thereof, or a trusted execution apparatus. A trusted execution apparatus may host a trusted execution environment. The apparatus may comprise memory access circuitry configured to retrieve a verification key from a memory. The memory access circuitry may comprise a hardware interface to a memory, such as for example at least part of a memory access bus. The memory may be comprised in the apparatus, or the memory may be external to the apparatus. The apparatus may comprise communication circuitry configured to receive a message. The communication circuitry may comprise, for example, an input or device of the apparatus. Where the apparatus comprises a mobile, the input device may comprise a radio receiver. Where the apparatus comprises a control device or trusted execution apparatus, the input device may comprise an input or output port of the control device or trusted execution apparatus. An input or output port may comprise a serial or parallel communication port, for example. In some embodiments, the communications circuitry performs memory access functions and the apparatus doesn't comprise separate memory access circuitry.

[0035] The apparatus may further comprise execution circuitry which may be configured to determine, using the verification key, whether the message is authentic. The determination may comprise verifying a digital signature of the message with the verification key. The execution circuitry may comprise, for example, at least one processing core. The execution circuitry may be configured according to von Neumann, Harvard or modified Harvard architecture, for example. In response to the message being determined to be authentic and to comprise an instruction to intercept a direct D2D communication, the execution circuitry is further configured to render the apparatus capable of storing, or causing storing, at least in part content of the direct D2D communication in at least one of the apparatus and the memory. In some embodiments, the apparatus does not determine whether the message is authentic, in other words the verifying of the digital signature is absent in some embodiments. In some embodiments, instead of content, or in addition to content, metadata relating to the D2D communication is stored. Metadata may comprise, for example, information identifying participants of the D2D communication and/or a duration of the D2D communication.

[0036] In some embodiments, in response to the message being determined to be authentic and to not comprise an instruction to intercept the direct device-to-device communication, the execution circuitry is further configured to cause the communication circuitry to indicate acceptance of the direct device-to-device communication. The acceptance may be indicated to a main processor of a mobile, for example. The indication of acceptance may comprise a response to a nonce comprised in the message. In some embodiments, the indication of acceptance and response to the nonce are caused to be transmitted in separate messages. In some embodiments, the nonce and response to the nonce are absent.

[0037] In some embodiments, the message comprises an encryption key, and the execution circuitry is configured to